

Robustness of interdependent networks under targeted attack

Xuqing Huang,¹ Jianxi Gao,^{1,2} Sergey V. Buldyrev,³ Shlomo Havlin,⁴ and H.Eugene Stanley¹

¹*Center for Polymer Studies and Department of Physics,*

Boston University, Boston, MA 02215 USA

²*Department of Automation, Shanghai Jiao Tong University,*

800 Dongchuan Road, Shanghai, 200240, PR China

³*Department of Physics, Yeshiva University, New York, NY 10033 USA*

⁴*Minerva Center and Department of Physics,*

Bar-Ilan University, 52900 Ramat-Gan, Israel

Abstract

When an initial failure of nodes occurs in interdependent networks, a cascade of failure between the networks occurs. Earlier studies focused on random initial failures. Here we study the robustness of interdependent networks under targeted attack on high or low degree nodes. We introduce a general technique and show that the *targeted-attack* problem in interdependent networks can be mapped to the *random-attack* problem in a transformed pair of interdependent networks. We find that when the highly connected nodes are protected and have lower probability to fail, in contrast to single scale free (SF) networks where the percolation threshold $p_c = 0$, coupled SF networks are significantly more vulnerable with p_c significantly larger than zero. The result implies that interdependent networks are difficult to defend by strategies such as protecting the high degree nodes that have been found useful to significantly improve robustness of single networks.

Modern systems due to technological progress are becoming more and more mutually coupled and depend on each other to provide proper functionality [1–3]. Social disruptions caused by recent disasters, ranging from hurricanes to large-scale power outages and terrorist attacks, have shown that the most dangerous vulnerability is hiding in the many interdependencies across different networks [4]. The question of robustness of interdependent networks has recently become of interest [5–8]. In interdependent networks, nodes from one network depend on nodes from another network and vice versa. Consequently, when nodes from one network fail they cause nodes in the other network to fail too. When some initial failure of nodes happens, this may trigger a recursive process of cascading failures that can completely fragment both networks.

Recently, a theoretical framework was developed [7] to study the process of cascading failures in interdependent network caused by *random* initial failure of nodes. They show that due to the coupling between networks, interdependent networks are extremely vulnerable to random failure. However, when we consider real scenarios, initial failure is mostly not random. It may be due to a *targeted attack* on important central nodes. It can also occur to low central nodes because important central nodes are purposely defended, e.g. in internet networks, heavily connected hubs are purposely more secured. Indeed, it was shown that targeted attacks on high degree nodes [9–13] or high betweenness nodes [14] in *single* networks have dramatic effect on their robustness. The question of robustness of *interdependent* networks under targeted attack or defense has not been addressed.

In this Letter, we develop a mathematical framework for understanding the robustness of interdependent networks under initial targeted attack which depends on degree of nodes. The framework is based on a general technique we develop to solve targeted attack problems in networks by mapping them to random attack problems. A value $W_\alpha(k_i)$ is assigned to each node, which represents the probability that a node i with k_i links is initially attacked and become inactive. We focus on the family of functions [12]

$$W_\alpha(k_i) = \frac{k_i^\alpha}{\sum_{i=1}^N k_i^\alpha}, -\infty < \alpha < +\infty. \quad (1)$$

When $\alpha > 0$, nodes with higher degree are more vulnerable and those nodes are intentionally attacked, while for $\alpha < 0$, nodes with higher degree are defended and so have lower probability to fail. The case $\alpha = 0$, $W_0 = \frac{1}{N}$, represents the random removal of nodes [7] and the case $\alpha \rightarrow \infty$ represents the targeted attack case where nodes are removed strictly

in the order from high degree to low degree. For the $\alpha < 0$ case, nodes with zero degree should be removed before analysis begins.

Our model consists of two networks, A and B, with the same number of nodes, N . The N nodes in each network are connected to nodes in the other network by bidirectional dependency links, thereby establishing a one-to-one correspondence. The functioning of a A-node in network A depends on the functioning of the corresponding B-node in network B and vice versa. Within each network, the nodes are randomly connected with degree distributions $P_A(k)$ and $P_B(k)$ respectively. We begin by studying the situation where only network A is attacked. We initially remove a fraction, $1 - p$, of the A-nodes of network A with probability $W_\alpha(k_i)$ (Eq.(1)) and remove all the A-links that connect to those removed nodes. As nodes and links are sequentially removed, network A begins to fragment into connected components. Nodes that are not connected to the giant component are considered inactive and are removed. Owing to the dependence between the networks, all the B-nodes in network B that are connected to the removed A-nodes in network A are then also removed. Network B also begins to fragment into connected components and only the nodes in the giant component are kept. Then network B spreads damage back to network A. The damage is spreaded between network A and B, back and forth until they completely fragment or arrive to a mutually connected component and no further removal of nodes and links occurs.

The main idea of our approach is to find an equivalent network A' , such that the *targeted* attack problem on interdependent networks A and B can be solved as a *random* attack problem on interdependent networks A' and B . We start by finding the new degree distribution of network A after removing, according to Eq.(1), $1 - p$ fraction of nodes but before the links of the remaining nodes which connect to the removed nodes are removed. Let $A_p(k)$ be the number of nodes with degree k and $P_p(k)$ be the new degree distribution of the remaining fraction p of nodes in network A ,

$$P_p(k) = \frac{A_p(k)}{pN}. \quad (2)$$

When another node is removed, $A_p(k)$ changes as

$$A_{(p-1/N)}(k) = A_p(k) - \frac{P_p(k)k^\alpha}{< k(p)^\alpha >}, \quad (3)$$

where $< k(p)^\alpha > \equiv \sum P_p(k)k^\alpha$. In the limit of $N \rightarrow \infty$, Eq.(3) can be presented in terms of

derivative of $A_p(k)$ with respect to p ,

$$\frac{dA_p(k)}{dp} = N \frac{P_p(k)k^\alpha}{\langle k(p)^\alpha \rangle}. \quad (4)$$

Differentiating Eq.(2) with respect to p and using Eq.(4), we obtain

$$-p \frac{dP_p(k)}{dp} = P_p(k) - \frac{P_p(k)k^\alpha}{\langle k(p)^\alpha \rangle}, \quad (5)$$

which is exact for $N \rightarrow \infty$. In order to solve Eq.(5), we define a function $G_\alpha(x) \equiv \sum_k P(k)x^{k^\alpha}$, and substitute $f \equiv G_\alpha^{-1}(p)$. We find by direct differentiation that [20]

$$P_p(k) = P(k) \frac{f^{k^\alpha}}{G_\alpha(f)} = \frac{1}{p} P(k) f^{k^\alpha}, \quad (6)$$

$$\langle k(p)^\alpha \rangle = \frac{f G'_\alpha(f)}{G_\alpha(f)}, \quad (7)$$

satisfy the Eq.(5). With this degree distribution, the generating function of the nodes left in network A before removing the links to the removed nodes is

$$G_{Ab}(x) \equiv \sum_k P_p(k)x^k = \frac{1}{p} \sum_k P(k)f^{k^\alpha}x^k. \quad (8)$$

On the other hand, the fraction of the original links that connect to the nodes left is

$$\tilde{p} \equiv \frac{pN \langle k(p) \rangle}{N \langle k \rangle} = \frac{\sum_k P(k)k f^{k^\alpha}}{\sum_k P(k)k}, \quad (9)$$

where $\langle k \rangle$ is the average degree of the original network A , $\langle k(p) \rangle$ is the average degree of remaining nodes before the links that are disconnected are removed. So the generating function of the new degree distribution of the nodes left in network A after their links to the removed nodes are also removed is [21]

$$G_{Ac}(x) \equiv G_{Ab}(1 - \tilde{p} + \tilde{p}x). \quad (10)$$

The only difference in the cascading process under *targeted* attack from the case under *random* attack is the first stage where the initial attack is exerted on the network A . If we find a network A' with generating function $\tilde{G}_{A0}(x)$, such that after a random attack with $(1-p)$ fraction of removed, the generating function of nodes left in A' is the same as $G_{Ac}(x)$, then the targeted attack problem on interdependent networks A and B can be solved as a random attack problem on interdependent networks A' and B . We find $\tilde{G}_{A0}(x)$ by solving the equation $\tilde{G}_{A0}(1 - p + px) = G_{Ac}(x)$ and from Eq.(10),

$$\tilde{G}_{A0}(x) = G_{Ab}(1 + \frac{\tilde{p}}{p}(x - 1)). \quad (11)$$

Up to now, we have mapped the problem of cascade of failures of nodes in interdependent networks caused by initial *targeted* attack to the problem of *random* attack. We can see that the evolution of equations only depends on the generating function of network A , but not on any information about how the two networks interact with each other. Thus, this approach can be generally applied to study both single networks and other interdependent network models.

Next we can apply the framework developed in Ref. [7], $g_A(p) = 1 - \tilde{G}_{A0}[1 - p(1 - f_A)]$, where f_A is a function of p that satisfies the transcendental equation $f_A = \tilde{G}_{A1}[1 - p(1 - f_A)]$. Analogous equations exist for network B . As the interdependent networks achieve a mutually connected giant component, the fraction of nodes left in giant component is p_∞ . The system satisfies the equations

$$\begin{aligned} x &= pg_A(y), \\ y &= pg_B(x), \end{aligned} \tag{12}$$

where the two unknown variables x and y satisfy $p_\infty = xg_B(x) = yg_A(y)$. Eliminating y from these equations, we obtain a single equation

$$x = pg_A[pg_B(x)]. \tag{13}$$

The critical case ($p = p_c$) emerges when both sides of this equation have equal derivatives,

$$1 = p^2 \frac{dg_A}{dx}[pg_B(x)] \frac{dg_B}{dx}(x)|_{x=x_c, p=p_c}. \tag{14}$$

which, together with Eq.(13), yields the solution for p_c and the critical size of the giant mutually connected component, $p_\infty(p_c) = x_c g_B(x_c)$. In general, there is no explicit expression as a solution and p_c and x_c can be found numerically.

We now analyze the specific classes of Erdős-Rényi (ER) [15, 16] and scale-free (SF) [17–19] networks. The lines in Fig. 1 represent the critical thresholds, p_c , for coupled coupled SF networks with different α obtained by solutions of Eq.(13) and Eq.(14), which are in excellent agreement with simulations. Several conclusions from Fig. 1 are as follows: (i) Remarkably, while p_c for a single SF network approaches to 0 quickly when α becomes zero or negative (see also [12]), p_c for interdependent networks is non-zero for the entire range of α (Fig. 1(a)). This follows from the fact that failure of the least connected nodes in one network may lead to failure of well connected nodes in the other network, which makes interdependent networks significantly more difficult to protect compared to a single

network. (ii) targeted attacks ($\alpha > 0$) and defense strategies ($\alpha < 0$) are more effective for interdependent networks with broader degree distributions. In Fig. 1(b), comparing the lines of $\lambda = 2.5$, $\lambda = 2.8$ and $\lambda = 3.4$ with $m = 2$, one can see that the lower is λ the more sensitive is p_c to the change of α . Accordingly, robustness of interdependent networks with broader degree distributions decreases more under the same targeted attacks.

Simplified forms for $G_{Ab}(x)$, $G_{Ac}(x)$ and $\tilde{G}_{A0}(x)$ from Eqs.(8),(10) and (11) exist when $\alpha = 1$,

$$G_{Ab}(x) = \frac{1}{p} \sum_k P(k) f^k x^k = \frac{1}{p} G_{A0}(fx), \quad (15)$$

$$G_{Ac}(x) = \frac{1}{p} G_{A0}(f(1 - \tilde{p} + \tilde{p}x)), \quad (16)$$

$$\tilde{G}_{A0}(x) = \frac{1}{p} G_{A0}\left(\frac{\tilde{p}}{p} f(x - 1) + f\right). \quad (17)$$

where $G_{A0}(x)$ is the original generating function of the network A, $f = G_{A0}^{-1}(p)$ and $\tilde{p} = \frac{G'_{A0}(f)}{G'_{A0}(1)} f$.

Explicit solutions of percolation quantities exist for the case of interdependent Erdős-Rényi networks, when $\alpha = 1$ and both of the two networks are initially attacked simultaneously. The two networks originally have generating functions $G_{A0}(x)$ and $G_{B0}(x)$. Initially, $(1 - p_1)$ and $(1 - p_2)$ fraction of nodes are targeted (according to Eq. (1) and $\alpha = 1$) and removed from network A and B respectively. Similarly, we start by finding the equivalent networks A' and B' such that a fraction $(1 - p_1 p_2)$ of random initial attack on both of the networks has the same effect as $(1 - p_1)$ and $(1 - p_2)$ fraction of nodes are intentionally removed from network A and network B respectively. After removal of initially failed nodes and all the links that connect to the removed nodes, according to Eq.(16), the generating function of the nodes left in network A is

$$G_{Ac}(x) = \frac{1}{p_1} G_{A0}(f_1(1 - \tilde{p}_1 + \tilde{p}_1 x)), \quad (18)$$

where $f_1 \equiv G_{A0}^{-1}(p_1)$, $\tilde{p}_1 \equiv f_1 \frac{G'_{A0}(f_1)}{G'_{A0}(1)}$. Furthermore, $(1 - p_2)$ fraction of the remaining A-nodes are randomly removed. Because each remaining A-node's corresponding B-node in network B has a possibility $(1 - p_2)$ to be initially attacked, which leads to fail this A-node. The generating function of the nodes left in network A is

$$G_{Ad}(x) \equiv G_{Ac}(1 - p_2 + p_2 x) = \frac{1}{p_1} G_{A0}(f_1 + \tilde{p}_1 f_1 p_2 (x - 1)). \quad (19)$$

Now we can find the generating function of the equivalent network A' by $\tilde{G}_{A0}(1 - p_1 p_2 + p_1 p_2 x) = G_{Ad}(x)$:

$$\tilde{G}_{A0}(x) = \frac{1}{p_1} G_{A0}(\frac{\tilde{p}_1}{p_1} f_1(x-1) + f_1). \quad (20)$$

The same holds for network B' .

For ER networks, the generating function is $G_0(x) = e^{<k>(x-1)}$ [21], so $f_1 = \frac{\ln(p_1)}{<k>_1} + 1, f_2 = \frac{\ln(p_2)}{<k>_2} + 1$, $\tilde{G}_{A0}(x) = \tilde{G}_{A1}(x) = e^{<k>_1 f_1^2(x-1)}$ and $\tilde{G}_{B0}(x) = \tilde{G}_{B1}(x) = e^{<k>_2 f_2^2(x-1)}$. From Eq.(12),

$$\begin{aligned} x &= p_1 p_2 g_A(y) = p_1 p_2 (1 - f_A), \\ y &= p_1 p_2 g_B(x) = p_1 p_2 (1 - f_B), \end{aligned} \quad (21)$$

where

$$\begin{aligned} f_A &= e^{<k>_1 f_1^2 y (f_A - 1)}, \\ f_B &= e^{<k>_2 f_2^2 x (f_B - 1)}. \end{aligned} \quad (22)$$

In the case $<k>_1 = <k>_2 = <k>$ and $p_1 = p_2 = p$, we find that

$$p_\infty = p^2 (1 - e^{<k> f^2 p_\infty}). \quad (23)$$

where $f_1 = f_2 \equiv f = \frac{\ln(p)}{<k>} + 1$, and p_c satisfies relation:

$$<k> p_c^2 f_c = 2.4554, \quad (24)$$

with $f_c = \frac{\ln(p_c)}{<k>} + 1$. Fig. 2 shows that the simulation confirms well the theory. Compared to the case of random attack on one network, where $p_c = 2.4554 / <k>$ [7], in Eq.(24), the factor f_c reflects the effect of targeted attack on high degree nodes to increase p_c . The term p_c^2 in Eq.(24) is since we are initially attacking both networks simultaneously instead of only attacking one network. Indeed for the case of initial random attack on two networks simultaneously, from Eq.(21) and $f_A = e^{<k>_1 y (f_A - 1)}$, $f_B = e^{<k>_2 y (f_B - 1)}$ [7] we obtain $<k> p_c^2 = 2.4554$.

In summary, we developed a theoretical framework for understanding the robustness of interdependent networks under targeted attacks on specific degree nodes. We introduce a method and show that targeted-attack problems in networks can be mapped to random-attack problems by transforming the networks which are under initial attack. It provides a routine method (if the random-attack case is solvable) to study the targeted-attack problems in both single networks and randomly connected and uncorrelated interdependent networks, i.e. (i) the case of three or more interdependent networks, (ii) the case of partially coupled

interdependent networks, (iii) the case in which a node from network A can depend on more than one node from network B . By applying the method, we find that in contrast to single networks, when the highly connected nodes are defended ($\alpha < 0$), the percolation threshold p_c has a finite non-zero value which is significantly larger than zero. For example, when the degrees of all nodes are known and nodes can only be damaged from lower degree to high degree ($\alpha \rightarrow -\infty$), $p_c \approx 0.46$ for coupled SF networks with $\lambda = 2.8$ and $\langle k \rangle = 4$ while p_c for the same single SF network is 0 (Fig. 1). The implications of the present study are dramatic. The current methods applied to design robust networks and improve the robustness of current networks, i.e. protecting the high degree nodes, need to be modified to apply to interdependent network systems.

-
- [1] J.C. Laprie, *et al.* Lect. Notes Comput. Sci. **54**, 4680 (2007).
 - [2] S. Panzieri & R. Setola, Int. J. Model. Ident. Contr. **3**, 69 (2008).
 - [3] V. Rosato, *et al.* Int. J. Crit. Infrastruct. **4**, 63 (2008).
 - [4] S.E. Chang, The Bridge **39**, 36 (2009). S.M. Rinaldi, *et al.* IEEE Control Syst. Mag. **21** 11 (2001).
 - [5] E.A. Leicht & M. D'Souza, e-print arXiv: 0907.0894v1 (2009).
 - [6] A. Vespignani, Nature (London) **464**, 984 (2010).
 - [7] S.V. Buldyrev, *et al.* Nature (London) **464**, 1025 (2010).
 - [8] R. Parshani, *et al.* Phys. Rev. Lett. **105**, 048701 (2010).
 - [9] R. Albert, H. Jeong and A.L. Barabási, Nature **406**, 378 (2000).
 - [10] D.S. Callaway, *et al.* Phys. Rev. Lett. **85**, 5468 (2000).
 - [11] R. Cohen, *et al.* Phys. Rev. Lett. **86**, 3682 (2001).
 - [12] L.K. Gallos, *et al.* Phys. Rev. Lett. **94**, 188701 (2005).
 - [13] A.A. Moreira, *et al.* Phys. Rev. Lett. **102**, 018701 (2009).
 - [14] P. Holme, *et al.* Phys. Rev. E **65**, 056109 (2002).
 - [15] P. Erdős & A. Rényi Publ. Math. **6**, 290 (1959). Publ. Math. Inst. Hung. Acad. Sci. **5**, 17 (1960).
 - [16] B. Bollobás, *Random Graphs* (Academic, London, 1985).
 - [17] A.L. Barabási & R. Albert, Science **286**, 509 (1999).

- [18] G. Caldarelli & A. Vespignani, *Large Scale Structure and Dynamics of Complex Webs* (World Scientific, 2007).
- [19] S. Havlin & R. Cohen, *Complex Networks: Structure, Robustness and Function* (Cambridge Univ. Press, England, 2010).
- [20] J. Shao, *et al.* Phys. Rev. E **80**, 036105 (2009).
- [21] M.E.J. Newman, Phys. Rev. E **66**, 016128 (2002).

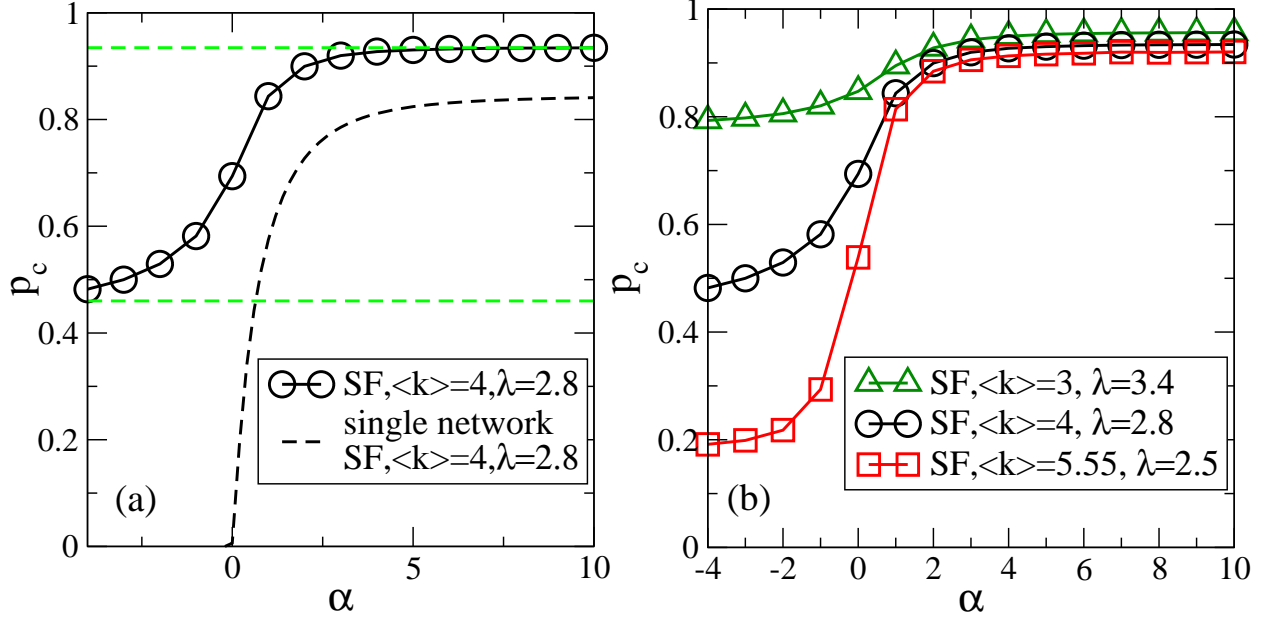


FIG. 1: (a) Dependence of p_c on α for SF single and interdependent networks with average degree $\langle k \rangle = 4$. The lower cut-off of the degree is $m = 2$. The horizontal lines represent the upper and lower limits of p_c . The black dashed line represents p_c for SF free network. (b) Values of p_c vs α for SF interdependent networks with different λ and lower cut-off $m = 2$.

The λ in the legends of both the graphs are approximate numbers.

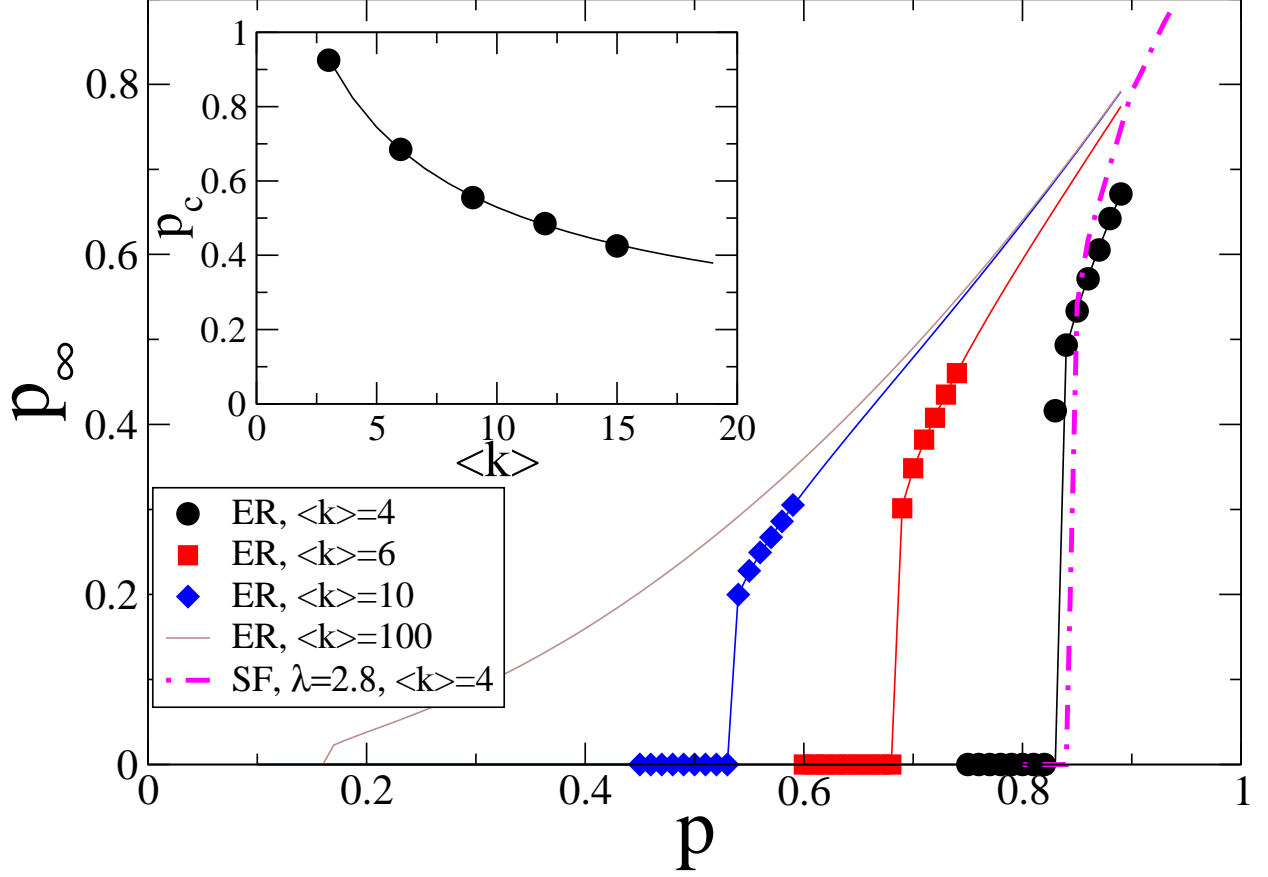


FIG. 2: Values of p_∞ vs p when both networks are initially attacked. Both networks in the interdependent networks are ER or SF networks with the same average degree. The symbols represent simulation data ($N = 10^6$ nodes). The solid lines are theoretical predictions, Eq.(23). The dashed line represents simulation data for interdependent scale-free networks with $\lambda = 2.8, \langle k \rangle = 4$. All results are for $\alpha = 1$. Inset: Values of p_c vs average degree of ER networks. The symbols represent simulation data, while the line is the theory, Eq.(24).